

REMARKS

This response is a full and complete response to the Office Action mailed April 5, 2006. In the present Office Action, the Examiner has noted that claims 1-31 are pending, that claims 1-3, 10-12, 20-23, and 31 stand rejected under 35 U.S.C. §103, that claims 4, 13, and 24 are objected to, and that claims 4-9, 13-19, and 24-30 would be allowable if rewritten in independent form.

By this response, claims 1, 3, 4, 12, 13, 21, 22, and 24 have been amended to correct typographical errors, to provide antecedent basis, and to make editorial changes. These amendments introduce no new matter and they are believed to be supported by the original application. These amendments are not believed to narrow the scope of the claims. Accordingly, it is believed that prosecution history estoppel is inapplicable.

In view of both the amendments presented above and the following remarks, it is submitted that the claims pending in the application are novel. It is believed that this application is in condition for allowance.

ALLOWABLE SUBJECT MATTER

Assignee's representative thanks the Examiner for identifying claims 4-9, 13-19, and 24-30 as being allowable if rewritten in independent form including all the limitations of the base claim and any intervening claim. In light of the remarks below and the amendments above, it has been decided to defer without prejudice rewriting the claims in independent form to a later time in the prosecution, if at all.

OBJECTIONS TO THE CLAIMS

Claims 4, 13, and 24 have been objected to over the language "preceding the round key data word to be generated". The two former claims have been amended above to call for "preceding said one of the second plurality of the round key data words to be generated", while the latter claim has been amended to call for "preceding said one of the second/fourth plurality of the round key data words to be generated". As amended, claims 4, 13, and 24 are believed to identify the round key data word. In light of the amendments to the claims, it is submitted that the grounds of objection are obviated and that claims 4, 13, and 24 are allowable.

REJECTION UNDER 35 U.S.C. §102

Claims 1-6, 8-15, 17-25, and 27-29 stand rejected under 35 U.S.C. §103 as being unpatentable over U.S. Patent 6,052,466 to Wright (hereinafter referenced as "Wright") and further in view of U.S. Patent 5,159,633 to Nakamura (hereinafter referenced as "Nakamura") and U.S. Patent 6,192,129 to Coppersmith (hereinafter referenced as "Coppersmith"). This rejection is respectfully traversed.

Independent claim 1 calls for:

In an apparatus, a method of operation comprising:
generating in real time a first deciphering round key based on a deciphering key;
incrementally deciphering a ciphered text for a first round using the real time generated first deciphering round key to generate a partially deciphered text;
generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for a said first round is being performed; and
incrementally deciphering the partially deciphered text for a second round using the real time generated second deciphering round key.

Wright appears to teach encryption of data packets using a sequence of private keys generated from a public key exchange. Each data packet is enciphered/deciphered using a

stream cipher produced by a particular private key called a secondary key. The data packet is enciphered or deciphered completely after a single application of the stream cipher produced by the secondary key. There is no teaching or remote suggestion in Wright concerning incremental deciphering.

Wright appears to teach incrementing an index and a page number for his various secondary keys. But Wright's incrementing is not to be confused with "incremental deciphering."

Incremental deciphering refers to an operation and/or process used in block encryption/decryption as opposed to stream encryption/decryption. It is to be understood that incremental deciphering is the deciphering operation that takes place in a particular round of deciphering. The deciphering is incremental because a round key can only partially decipher the ciphered text block. Application of a multiplicity of round keys, each in its own particular round of deciphering, to the same text block in its successively partially deciphered state can ultimately produce the completely deciphered text block.

But incremental deciphering is not taught by Wright, separately or in combination with the other references. Wright clearly uses only one secondary key to completely decipher or encipher a packet. See *Wright*, col. 8, lines 8-16. When the packet is completely deciphered by the stream cipher produced by the single secondary key, a new packet enters the decryption apparatus for deciphering using a different stream cipher produced by a different secondary key. Wright never even remotely suggests the use of multiple keys in successive rounds to decipher a single packet. Wright shows no motivation for including multiple keys in successive rounds to decipher a single packet. As a result, Wright fails to teach, show, or suggest incremental deciphering as claimed in the present application.

Nakamura was added to the combination to provide a sense of real-time operation. But Nakamura appears to teach real-time operation for the encryption operation only. Nakamura evidences no concern for real-time decryption operation, in general, or real-time round key generation for decryption, in particular. Nakamura is completely silent about the manner in which keys are generated for decryption. As a result, the addition of Nakamura to Wright and Coppersmith fails to teach, show, or suggest "generating in real time a first deciphering round key based on a deciphering key" and "generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for a said first round is being performed", as claimed in the present application.

Coppersmith was added to the combination to provide a sense of rounds. Coppersmith appears to involve block encryption/decryption and the use of round keys, called sub-keys, in different rounds to encrypt/decrypt text. Coppersmith even appears to describe the prior generation and, if desired, the storage of the round keys for encryption only. See *Coppersmith, Figs. 5a & 5b and col. 20, lines 60-67*. But Coppersmith teaches nothing about "generating in real time a second deciphering round key based, at least in part, on said generated first deciphering round key while said incremental deciphering for a said first round is being performed", as claimed in the present application. Coppersmith is completely silent about the generation process for his sub-keys (round keys) and, as a result, the time at which particular sub-keys are generated. Thus, even though Coppersmith appears to teach the use of rounds, the addition of Coppersmith to the combined teachings of Wright and Nakamura cannot cure the deficiencies of those teachings.

As a result, the combination of Wright, Nakamura, and Coppersmith fail to teach, show, or suggest all the elements of claim 1. Since this combination of references does not teach all

the elements of claim 1, it is submitted that claim 1 would not have been obvious to a person of ordinary skill in the art upon a reading of this combination of references. Therefore, it is believed that claim 1 is allowable under 35 U.S.C. §103.

Claims 2-3 depend from claim 1, either directly or indirectly, and include all the limitations thereof. In view of the remarks above for base claim 1, it is submitted that claims 2-3 are allowable under 35 U.S.C. §103.

Claims 10 and 20 and the claims dependent therefrom, contain limitations similar to those discussed above with respect to claim 1. Therefore, in view of the remarks above, it is submitted that claims 10-12, 20-23, and 31 are allowable under 35 U.S.C. §103.

CONCLUSION

In view of the amendments and remarks above, it is submitted that this application is in condition for allowance. Reconsideration and allowance are respectfully solicited.

If, however, the Examiner believes that there are any unresolved issues requiring adverse action in any of the claims now pending in the application, it is requested that the Examiner telephone Gregory C. Ranieri, Esq. at (503) 439-6500 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Dated: Sept. 5, 2006

Respectfully submitted,

Gregory C. Ranieri
Gregory C. Ranieri
Registration No. 29,695
Attorney for Assignee

Customer No. 43831
Berkeley Law and Technology Group, LLC
1700 NW 167th Place, Suite 240
Beaverton, OR 97006
503-439-6500